Information Technology Resource Management Council (ITRMC)
Special Teleconference Meeting Minutes
(Approved by Council December 7, 2001)

October 2, 2001
4:00 to 4:40 p.m., Conference Room 155, LBJ Building
650 West State Street, Boise, Idaho

The October 2, 2001 meeting of the Information Technology Resource Management Council (ITRMC) was held in Conference Room 155 of the LBJ Building, 650 West State Street, Boise, Idaho.

CALL TO ORDER, WELCOME

Pam Ahrens, Council Chairman, who welcomed members and guests present, called the meeting to order.

ATTENDANCE

Members/Designates Present:
Mrs. Pam Ahrens, Chairman
Mr. Dwight Bower, Agency Executive Office
Senator Hal Bunderson, Idaho Senate
Mr. Ken Harward, Local Gov. Representative
Dr. Marilyn Howard, Department of Education
Mrs. Mary Elizabeth Jones, Rural Rep.
Mr. Karl Kurtz, Agency Executive Officer
Representative Bert Marley, Idaho House
Mr. Roger Parks, Private Industry Representative
Mr. John Peay, Judicial Representative
Mr. J.D. Williams, State Controller
Mr. Steve Wilson, Idaho Tax Commission

*Designate

Absent Members:
Representative Lee Gagner, Idaho House
Senator Clint Stennett, Idaho Senate
Mr. Gary Stivers, State Board of Education
Colonel Ed Strickfaden, Idaho State Police

Others Present:
Mr. Nathan Bentley, ITRMC Staff
Mr. Rich Elwood, ITRMC Staff
Mr. Bill Farnsworth, ITRMC Staff
Mr. Don Fournier, ITRMC Staff
Ms. Emily Gales, ITRMC Staff
Mr. Dan Hawkins, Department of Education
Mr. Charlie Wright, Dept. of Health and Welfare

BACKGROUND

Chairman Pam Ahrens provided background on the purpose of today's meeting. On September 27, 2001, Governor Kempthorne issued **Executive Order 2001-13** directing agencies across state government to create disaster preparedness plans to evaluate issues that may impact the state in a time of some type of incident or threat. One of the issues that came to light was not only protection of facilities, employees and services provided to the citizens of Idaho, but the state's wide area network (WAN). It has fallen on the ITRMC as the information technology (IT) policy setting group for the State of Idaho to develop the guidelines of how the state addresses security of its data and telecommunications networks. There is an area we have come to consensus on since work on the policies and standards by this Council have commenced. It has become rather apparent that it would be helpful to have the Council's approval on these standards so that as we send out guidelines and assistance to state agencies, ITRMC's intent regarding security issues will be known. It is important to have these in place as we move forward, Ahrens said.

ITRMC UPDATE

Chairman Ahrens introduced and welcomed Steve Wilson, Idaho Tax Commission, as the newest member of ITRMC, appointed by Governor Kempthorne.

ITRMC IT ENTERPRISE STANDARD 3000 – NETWORK & TELECOMMUNICATIONS

Chairman Ahrens asked Rich Elwood, Statewide IT Coordinator, ITRMC Staff, to discuss Enterprise Standard 3000, categories 3100 and 3110. Mr. Elwood explained that the standards to be covered were prepared for review by various IT managers of the major agencies in the state. The ITRMC Staff has received feedback, as represented in these standards. These standards were to be presented for approval at ITRMC's October 17th teleconference meeting, but have been brought forth today as indicated by Chairman Ahrens.

Category: 3100 Network Services – Internet/Intranet Web Server and
Category: 3110 Network Services – Internet/Intranet Web Browser

Categories 3100 and 3110 are standards discussed in conjunction because they are essentially de facto standards for the state in that most state agencies are already currently using them. By standardizing on these two elements of software, we are able to provide an infrastructure background for the development of applications that may use web server and web browser products, simplify the development effort, and provide agencies with a common platform to develop on across the state.

Steve Wilson made note that in Category 3110, Microsoft Internet Explorer (IE) version 5.x was listed under Approved Products, but that IE version 6 had already been issued. This is because IE version 5.5 is in use and available. These standards are living and an annual review is noted under this particular standard. Perhaps, though, it should be reviewed semi-annually, said Elwood.

Mr. Elwood asked Don Fournier, ITRMC Policy Analyst, to go over categories 3120 – 3220.

Mr. Fournier advised categories 3120, 3200, 3210 and 3220 are security standards that are part of a larger framework/security architecture. All four are either primarily in use by state agencies or are applications/security pieces that are on the leading edge of security currently being put into use.

Category: 3120 Network Services – Data/Network Integrity

Category 3120 falls into the category of a new standard that is currently being deployed as part of the security framework. Given the analogy of security in a building/house, the data/network integrity system is the closed-circuit alarm system, collecting forensic evidence and information critical for both intrusion detection and investigation security. The industry leader in this space is Tripwire. A Tripwire system is currently being deployed on the shared infrastructure and has generally been accepted by agencies as the standard for this type of application.

J.D. Williams noted that Tripwire 2.2.1 for Linux was referred to under Approved Products, but that Linux was not listed under Approved Operating Systems. The Linux product was listed as an approved product in the anticipation of Linux products being used in the infrastructure in the future, said Fournier.

Category: 3200 Security – Firewall

The firewall products are already in place within the state network and at major agency interconnect points. The Check Point Firewall is being used at the state Internet POP (point of presence), within the state network, and by most major state agencies. The rationale for standardizing on the Check Point Firewall is to provide for the broadest possible support for the product, easy integration within the rest of the state's network, high level of expertise, and – should it be needed – the proprietary encryption features of the firewall can be utilized within the infrastructure. Check Point is recognized as the industry leader in firewall products, and by far, we have the largest amount of expertise in that arena, Fournier said. The IT managers have reviewed this, and consensus has been established that this is the best product in this space.

Currently, there is a state contract with Cisco. As noted by Steve Wilson, as long as Check Point is adopted as the standard, agencies will migrate to the standard, as they are able to do so.

Category: 3210 Security – Network Intrusion Detection System

For a network intrusion detection system, an analogy can be made to the burglar alarm system in a house. The network intrusion detection system is fairly new technology in the security arena. It analyzes traffic coming through the network and looks for signatures that might represent some kind of attack or unusual traffic pattern. The state has some very good success stories related to the approved product listed under this standard. During the Code Red and NIMDA events, the network intrusion detection systems deployed within the infrastructure and Internet POP, in combination with a similar device deployed in the Idaho State Insurance Fund, were able to correlate the events of the NIMDA worm very rapidly, and the State of Idaho was one of the first organizations to recognize that something unusual was happening. This is a very valuable technology in alerting us when there is something amiss and even more so when done in a centralized, coordinated fashion, as was during the recent events. The ITRMC Staff – as well as agency IT managers – strongly support this technology and propose it as a standard for intrusion detection.

Category: 3220 Security – Virtual Private Network

This last piece of the security framework standard deals with virtual private network (VPN) hardware and software. The products are the Check Point Gateway, Check Point SecuRemote and Check Point SecureClient. The Check Point VPN product works extremely well with the Check Point Firewall, and provides an excellent solution for enterprise and remote access to the state network.

All security products discussed will support the pieces to come in the future: PKI (Public Key Infrastructure), digital certificates and the secure remote access products.

MOTION TO APPROVE ITRMC STANDARDS 3000

Dwight Bower moved and Mary Elizabeth Jones seconded a motion to approve all categories associated with ITRMC Information Technology Enterprise Standard 3000 – Network and Telecommunications, and the motion passed unanimously.

DISCUSSION

Chairman Ahrens advised that ITRMC has other standards before it that may have some impact on security issues. Ahrens asked Rich Elwood to talk briefly about those standards, and entertained recommendations for other areas that need to be investigated. Elwood advised that the policies to be discussed at the next Council meeting, October 17th, deal with the use of the Internet, e-mail, and personal computers – all of which include some component of security. In addition, there are previously approved standards that have been rewritten. Those standards need to be reviewed and re-adopted by the Council. The ITRMC Staff will be re-prioritizing its efforts to develop a state **IT Security Policy**. The Staff is also accelerating work on a **Business Recovery Plan** guideline, providing agencies with a format for developing recovery plans in compliance with ITRMC Policy 2020 Business Recovery Planning (approved August 29th). This is a very critical component to both cyber and physical security. Sample information may be available for Council review at the October 17th meeting.

J.D. Williams mentioned the Controller's office had been working on a disaster recovery plan for about five years, and that it was not an easy process. There was more discussion regarding state and private sector security measures.

Mr. Williams questioned whom 'state' was referring to under item "K" of Policy 1050 – Employee Internet Use: '*The state has the right to inspect…*'. Rich Elwood advised 'state' refers to the agency that has files stored in secured areas of state networks, etc. or another designated agency with custody of such items. The word 'state' is used as opposed to naming specific agencies. This point should be clarified in policies 1050 and 1060 (item "G"), said Chairman Ahrens.

Williams then raised a question regarding item "F" of Policy 1060, noting that some supervisors do not mind if employees play computer games (those included with the operating system) on their

own time, such as lunch. Chairman Ahrens asked that this determination be designated by the agency, and that Policy 1060 be modified to reflect this. Mr. Elwood mentioned the intent of this item was to prevent employees from downloading games from the Internet that would take up a large amount of space on the network. Executive Order 98-05, issued by Governor Batt, as well as a proposed executive order currently before Governor Kempthorne, refers to the minimum level of standard and defers to the ITRMC for the responsibility of setting more stringent standards, if appropriate. The pending executive order before the governor is much more detailed than Executive Order 98-05.

ADJOURNMENT

As there was no new business to come before the Council at that time, Chairman Pam Ahrens thanked those in attendance and adjourned the meeting at 4:40 p.m. The next ITRMC meeting is scheduled for Wednesday, October 17, 2001 from 8:30 – 9:30 a.m. in the East Conference Room, Joe R. Williams Building. The 2001 Digital Government Boot Camp will be held on October 25th.

Respectfully submitted,

Emily Gales
ITRMC Assistant